Proceedings of International Web Conference "Cyber Security"
30th November 2022, Organized by Sbyte Technologies
Sponsored by INFISUM, USA.

Focus On Some Cyber Security Topics: Literature Based Study

DESAM SUDHAKAR REDDY, **M.Sc. (Chemistry), PGDEM,**
Author& Creator, Audio-visual Representation of Chemistry,AVC), Hyderabad, Telangana State

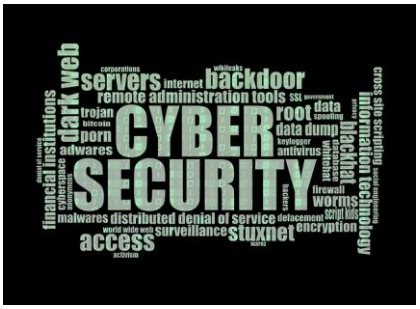
D.DEEPSHIKA
Class8, BVBVSchool, NIRD, Hyderabad

Abstract: **Cybersecurity is the practice of protecting systems, networks and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Globally, there is an explosive growth of internet, with its penetration estimated to be around 3.4 billion users (47% world population). Cyber Security is the practice of preventing cybercrime. Various types of cyber-attacks like phishing attacks, DDoS, password attacks, SQL & ransomware attacks are causing detrimental financial damage to the individual & industry.**

Key words: **Cloud Computing; Multi Tenancy; Control Of Cloud; Cloud Security; Deployment Models;**

INTRODUCTION

Over years, the internet has advanced phenomenally and transformed itself into coming age of Internet of Things (IOT), Big Data, Automation, Virtual and Augmented reality. With the evolution of technology, owing to greater benefits of internet, people have become more dependent on it. Internet, apart from providing enormous opportunities, it has also been epicentre for cybercrime, cyber security, and espionage. For the said reasons, protecting our gadgets, computers, laptops, and cloud data from cyber-attacks has gained significance. All sectors of government, business, industry, and academia is built on technological foundations we all are aware – Internet, Computes, Gadgets, Smart watches, Mobiles etc. In every computer, gadget, app, social media etc., important private information or data of public is stored. In this digital world with more products and services moved online, we all global citizens have in turn heavily dependent on them. Thus protecting our technological infrastructure and information system globally has even become more fundamental and utmost essential.

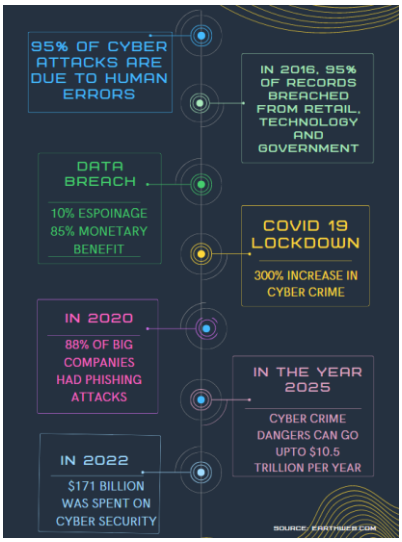


The Importance of Cyber Security

The world relies on technology more than ever before. As a result, digital data creation has surged. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization. A data breach can have a range of devastating consequences for any business. It can unravel a company's reputation through the loss of consumer and partner trust. The loss of critical data, such as source files or intellectual property, can cost a company its competitive advantage. Going further, a data breach can impact corporate revenues due to non-compliance with data protection regulations. It's estimated that, on average, a data breach costs an affected organization $3.6 million. With high-profile data breaches making media headlines, it's essential that organizations adopt and implement a strong cyber Security approach:

Cyber Crime: Globally, there is an explosive growth of internet, with its penetration estimated to be around 3.4 billion users (47% world population). The heavy exposure of computers, gadgets, and other machinery on web / internet, have enabled hackers to steal data, commit banking fraud bringing down websites, which is termed as cybercrime. Cyber Security is the practice of preventing cybercrime i.e., any form of unauthorized and malafide access to a PCs, Smart Phones, National Banking System, National Defence Network in the first place, minimizing its impact. Initially cyber space was primarily restricted to civilian usage, later its utility has spread to various important sectors of National importance like Banking Sector, National Information Technology and Defence sector etc. This increased prevalence of malicious cybercrimes by hackers has enabled breaches, posing extraordinary threat to the National Security, Foreign policy and even economy among all

nations across the world. As per recent studies, cyber-attacks were more prominent, largely targeted industries like manufacturing (28%), public administration (21%), professional businesses (14%), whileFinance and Health sectors were least affected.



Recent studies have also revealed that people clicking on phishing links sent by strangers, have become scapegoats of cybercrimes. This is clear indication that cyber security is not just about technological defences, but it is more do about the welfare of people, government, and Industry. Above statement emphasizes the need to recognize cyber threats as potential risk, as certaining the need to create awareness among common people, all sections of society and more importantly gain knowledge under digital literacy. Cyber-attacks are primarily financially motivated.

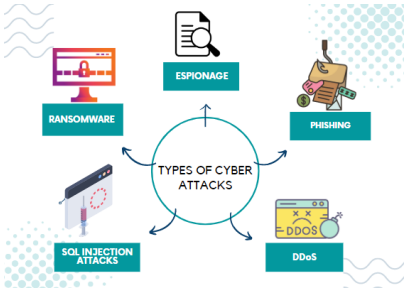
Types of Cyber Attacks

1) Phishing Attacks

It is one of the most prominent types of cyberattacks, which is also termed as social engineering attack.Using trustworthy emails or web pages, certain links are sent to individuals or organisation's mail accounts. Responding to such email by way of providing personal information (or) by clicking the links is termed as Phishing. Accessing this malware allows hackers gain access to confidential personal information and bank account credentials. This facilitates hacker steal money from victim either individual /organisations from their respective bank accounts.

For example, an organization employee Sudhakar receives an email stating that "Your password is expiring, please re-set the password by clicking following link." Once the individual clicks the link, entire personal information will be accessed by the cyber criminals. Phishing attacks may be prevented by following below mentioned steps:

- Emails received from unknown sources should be thoroughly scrutinized
- Password need to be updated on regular basis; anti-phishing toolbar will help.



2) Distributed Denial of Service Attacks (DDoS)

1. Distributed Denial of Service Attacks (DDoS): Bots are the services of media agency or hackers operated on social media networks which allow,enables to acquire personal information fromindividual'sprofile. Bots are fake accounts which automatically generate messages on social media platforms, emails etc. to advocate ideas & even acquire followers. Using thousands of bot accounts cybercriminals deny access to web page, without stealing data.

a. Example:

Rajesh sees an AD in Facebook, "BUFFET for 4 members@ INR450/-.Pleaseclick the link to generate coupon to avail this offer."Individual finds this as great opportunity to give surprise to his family members during the weekend. On processing the payment link, he finds no coupon is generated. On chatting with customer care, he receives the message *May be there is an issue in your computer*. We will refund the amount or else please install following software*. Trusting the chat, Rajesh installs the software, which enabled the hacker to extort entire money from his bank account.

Ways to prevent DDoS:

i) Understanding warning signs like slowing down of network, sporadic website shutdowns.

ii) Organisations need to prepare incident response plan, conducting training on DDoS preventive measures, bringing awareness to the workforce.

iii) Conducting traffic analysis.

3) Password Attack:

Using various password cracking tools like Abel, Hash cat etc., hacker cracks the individual's bank account. This allows the cyber criminals to steal money from bank accounts. Such attacks can be avoided by

i) Using strong alphanumeric passwords with special characters.

ii) Avoiding same passwords for different accounts.

iii) Updating password regularly will limit password attacks.

4) Vishing attacks:

During covid-19 pandemic, many organisations have switched their businesses to Virtual mode instead of physical mode. Owing to Lockdowns, strict Standard Operating Procedures (SOPs) like social distancing measures, frequent sanitation, has led to huge surge in the emergence of e-commerce companies, which has become blessing in disguise for hackers.

In Vishing attacks, hacker uses social media platforms and targets the individual by making personal calls, encouraging individuals, employees to disclose personal information.

5) SQL Injection Attack:

SQL means Structured Query Language, used by cyber criminals is usually intended to cause damage to the data driven websites. Hacker introduces a malicious code into the search box of website to access important information. This enables the attacker to view, edit as well as delete important data by gaining administrative access.

Websites can avoid SQL Injection Attack by using

i) IDS (Intrusion Detection System) and

ii) By incorporating Robust Validation Process.

6) Identity Theft:

It involves cyber criminals stealing of private information pertaining to individuals debit card or credit card. Normally villagers do not have proper knowledge in respect of operating ATM card to withdraw money, hence depend on others. Stranger pretends to help the villager, swipes the card, asks for password and says that the card is neither functional nor blocked. He owns similar fake card pertaining to set of banks, return the fake card to villager, extorts money immediately at other ATMS.

7) Watering Hole Attack:

In this attack, hacker's targets certain group of an organisation, wherein they frequently visit specific websites. Cyber criminals using malware infects the websites. When such websites are accessed by employees, computer gets infected, provides hacker remote access.

Watering Hole Attack may be prevented by using private browsing feature or VPN or Virtual Private Network. VPN delivers a secured network over internet, conceals online activity and acts as a shield for hackers.

8) Ransom ware Attacks:

Ransom ware generally targets the person who has fallen victim of cyber-attacks via phishing, with primarily intention to collect sensitive data and hold the information until one succumbs and process the payment demanded by hacker.

These attacks can be prevented by

i) Using antivirus software like Norton, McAfee to protect PC from malware

ii) Avoid clicking suspicious links

iii) Activating inbuilt OS firewall enables to filter traffic

iv) Updating OS & browsers on regular basis

9) Cybercrimes may be categorised into Financial & Vanity attacks

i) Financial attacks:

Hacks indulge in financial cyber-attacks, primarily intending to extract huge money apart from stealing personal information. For example, in January 2017, crypto.com - an online trading platform was hacked to extract & flush out more than 30 million USD in Crypto Currency.

ii) Vanity attacks:

Hackers primarily target tech giants, attacking to cause temporary halt in their services, without stealing information. The main intent is to prove a

point that big organisations are also vulnerable to cybercrime.

For instance, in one of the cyber-attacks of Microsoft, the company's Argue Dev ops servers were breached and even downloaded 37 GB of source code from cloud computing. Hence, the cyber-attack is aimed to damage the reputation of organizations.

10) The Internet of Things (IOT):

Various Electronic devices like smart TV's, webcam, latest refrigerators function only when these are connected to 24/7 internet.

Electronic devices have in built technology which encompasses hardware, software, data service in electric devices is called internet of things (IoT), thus are prone to limitless cyber-attacks. A successful attack on Industrial IoT devices will cause detrimental havoc, devastating the infrastructure, leading to financial losses which may in turn instigate organizations to lay off its workforce.

Internet Of Things (IoT)

11) Autonomous System:

Many organizations, industries are transforming their infrastructure with automation. For example, Driver less cars replacing conventional cars are stealing the lime light of future generations. Recently few accidents were reported in driverless cars, leading to loss of lives. Hackers have remotely misused music system then took control over car systems and demonstrated that autonomous systems are vulnerable to cyber-attacks. In 2015, 1.4 million jeep Cherokees were recalled owing to inadequacy of existing cyber security.

12) ATMS &Credit Cards:

During purchase of goods in supermarkets, customers generally use contactless credit cards or Wi-Fi enabled cards for payment of bills at Bill Counters. At the point of payment there is high probability of hacker indulging in cyber breach by way of accessing Credit card number, Expiry date and most importantly Card Verification Value (CVV) extract money.

13) CYBER WARFARE:

In recent part warfare between countries has occurred via, land, sea, and air. But, today a new domain of warfare called cyberspace has surfaced. This has enabled the hackers to commit cybercrime by accessing the automated systems installed at premier institutions like Railway network, Military Defence systems, National information technology and Space organisations. This provides ample opportunity to miscreants or terrorists to hack and access most precious information pertaining to transport facilities, disrupting communication system or national information technology assets that has many military implications. Now we are living in a world wherein countries may indulge in warfare conducted virtually through cyberspace. This cyber warfare may be detrimental, causing irreparable damages to physical world. Hence, cyber space warfare has been officially declared as 5th dimension of warfare.

14) Cyber-attacks on Infrastructure:

As the societies around the world begin to depend heavily on internet a technology, the probability of cyber-attacks increased thereby inflicting damage to infrastructure and national security system.

Few incidents of cyber-attacks on infrastructure include: In 2008, both US and Israel jointly design a Trojan horse malware (or) computer called STUXNET. This can propagate from one computer to another causing detrimental breach to a system without human intervention. Using STUXNET both the countries caused disruption to Iranian Nuclear Plant.

Data manipulation:

Data manipulation is a methodology in which structured data is organised, arranged in such a way to enable computer program to easily interpret. Data Manipulation can be used either to improve quality of data (or) even destroy it.

In cyber world, a backdoor refers to a method by which authorised and unauthorised users get access to data on a computer system (or) software application. Backdoor uses additional malware, enabling hackers to steal personal financial data and even hijack devices.

Using backdoors hackers control the firewall operating system code installed in computers. This allows cybercrimes to spy on data i.e., espionage causing detrimental effect to National Security.

Cloud Concerns':

In order to store huge database both companies as well as individuals are utilizing cloud spaces for various purposes. But even these cloud spaces may be prone to cyber-attacks with the possibility of causing detrimental damage to precious data.

Opportunities

Technology as wealth creation, technological advancements and their benefits, have created tremendous job opportunities globally, became the sources of wealth creation.

Ex: Google, Face book, YouTube.

Industry &Individual:

In majority of cybercrime cases, hackers usually target businesses and individuals using malware. These cyber-attacks incur huge financial losses to a tune of millions of dollars.

Ransom ware and Cryptoware:

Recently in 2016 we have all seen the prevalence of crypto ware which targeted both organizations & individuals.

Cyber criminals using ransom ware locked important data pertaining to enterprises and extorted ransom amounts to unlock encrypted files. Crypto locker is one such ransom ware, which is supposed to have extracted millions

Cyber Security opened new Job Opportunities:

With unprecedented growth in cybercrimes, across all sector including industry, it has become blessing in disguise for the hackers. Cyber security of many organizations has gained significance opening plethora of Job opportunities viz., Security Engineer, Security architect, Security analyst etc.

Collaboration:

Research and analysis of cybercrimes have revealed that hackers work together exceptionally well; working together in co-ordination enables them to develop new hacking techniques, selling private information, stolen data in open market. On the flipside, there is little co-operation between Government and Industry in respect of cyber-attacks.

Reason behind company's not revealing cyber-attacks incidents primarily because the news may create shock waves in the stock market, impacting their share value, in turn damaging their reputation. Keeping cyber-attack, a secret in turn helps cyber criminals to exploit and extort money. This asserts the need for organizations to gain knowledge, share the information of cyber-attacks among cyber professionals and other business partners enabling to take appropriate measures preventing such cybercrimes in near future.

Education and Awareness:

1) As most of the industries, government undergoing digital transformation, the incorporation of cyber security wing/department becomes inevitable. Inching and moving close to digital economy, we all need more engineers, programmers, mathematicians, data analysts, hardware experts and scientists.

2) With growing cyber-attacks looming across global industry, government needs to promote degrees exclusively in the disciplines viz.,

Cybercrimes, ICT cyber security at university level. Further, greater emphasis should be laid to inculcate strong fundamentals among school children in basic sciences like mathematics, physics, chemistry, more importantly laying special emphasis on STEM subjects likes science, Engineering, Technology, and coding

3) Proper steps need to be taken both by Government and Industry by way of framing policies, procedures to prevent and curtail cyber-attacks.

4) It is noticed that there is huge dearth of cyber security knowledge among Entrepreneurs, CEOs and Board members of many organizations.

5) Employees' role with regards to cyber security and alertness plays a critical role in curtailing the cyber-attacks caused to organization. This is mainly because smart phones in employee's pockets act as vectors, may be prone to data leaks caused by cyber-attacks, proving fatal to company. Hence, cyber security may be considered as a business risk.

Preventive measures for cyber-attacks

i) Complex pass words need to used using capital letters, numbers, symbol between sites and services. Password manager can be used if individual finds hard to remember many passwords.

ii) It is important to note that reputed banks never ask for password details over email (or) phone. Phishing emails should be recognized to avoid to cybercrimes.

iii) Pop-ups appearing while browsing internet should not be clicked. Further, pop ups promoting file downloads or installation of software should be avoided. Operating system (O.S) of computers should be regularly updated to prevent cyber-attacks.

iv) In Malls we all see different persons approaching us seeking phone number, email details in the name luring free gifts. Email and contact details are sold by these persons for huge amounts. Do not reveal one's personal information to anybody apart from close friends, as there is nothing called FREE.

CONCLUSION

In addition to established competitors, fintech companies often face doubts from financial regulators like issuing banks and the Federal Government. In July 2018, the Trump Administration issued a policy statement that allowed FinTech companies to apply for special purpose national bank charters from the federal Office of the Comptroller of the Currency. Federal pre-emption applies to state law regarding federally chartered banks. Data security is another issue regulators are concerned about because of the threat of hacking as well as the need to protect sensitive consumer and corporate financial data. Leading global fintech companies are proactively turning to cloud technology to meet increasingly stringent compliance regulations. The Federal Trade Commission provides free resources for corporations of all sizes to meet their legal obligations of protecting sensitive data. Several private initiatives suggest that multiple layers of defence can help isolate and secure financial data.

ACKNOWLEDGEMENTS

Authors hereby thank Dr. Sridhar Seshadri, Ex. Vice-Chancellor, for his continuous support, guidance, and mentorship. His comments while reviewing this paper for publication are highly appreciable and well taken to modify this final version.

REFERENCES

[1]. Centre for Strategic international Studies, techgenix.com, Cybersecurity: Threats, Challenges, Opportunities – ACS, https://www.acs.org.au › acs › acs-publications

[2]. "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2020.

[3]. "computer security | Definition & Facts | Britannica". www.britannica.com. Retrieved 12 July 2022.

[4]. "Computer Security and Mobile Security Challenges". researchgate.net. 3 December 2015. Archived from the original on 12 October 2016. Retrieved 4 August 2016.

[5]. "Cryptocurrencies: What Are They?". Schwab Brokerage.

[6]. "Cyber crime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.

[7]. "cybercrime | Definition". Encyclopaedia Britannica. Retrieved 25 May 2021.

[8]. "cybercrime | Definition, Statistics, & Examples | Britannica". www.britannica.com. Retrieved 14 December 2021.

[9]. "Email Security | Trellix". www.trellix.com. Retrieved 24 October 2022.

[10]. "EXP-SA: Prediction and Detection of Network Membership through Automated Hard Drive Analysis".

[11]. "Ghidra". Archived from the original on 15 August 2020. Retrieved 17 August 2020.

[12]. "How To Make A Mint: The Cryptography of Anonymous Electronic Cash". groups.csail.mit.edu. Archived from the original on 26 October 2017. Retrieved 11 January 2018.

[13]. "Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015. Retrieved 4 July 2016.

[14]. "Insurtech startups are leveraging rapid growth to raise big money". TechCrunch. April 20, 2021. Retrieved October 13, 2021.

[15]. "Is it a currency? A commodity? Bitcoin has an identity crisis". Reuters. 3 March 2020. Retrieved 25 January 2022.

